UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,659	06/25/2003	Bing Wang	08212/0200290-US0/NC28834	4744

53666 7590 04/28/2009
BRAKE HUGHES BELLERMANN LLP
c/o CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
OKEKE, IZUNNA	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
04/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/606,659	**Applicant(s)** WANG ET AL.	
	Examiner IZUNNA OKEKE	**Art Unit** 2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *26 January 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-6,8-10,17,21,24,25,30-38 and 41-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4-6, 8-10, 17, 21, 24-25, 30-38 and 41-43* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 01/26/2009 have been fully considered but they are not persuasive.

On Page 1 of applicant's argument and remarks, applicant argues that Waldin does not teach a hash value of the file and comparing a hash value of the file to a stored value. Waldin does implicitly teach hashing the file, storing the hash value of the file and comparing the hash value to a stored hash value (See Waldin, Col 2, Line 57-63 and Col 3, Line 21-34). Waldin teaches that this method of comparing hash values has been used in prior arts (See Waldin, Col 2, Line 57-63 and Col 3, Line 21-34), but his invention improves on its deficiency by comparing the size of the hashed files because an attacker or virus can be implanted within the file after the hash has been taken and the comparison of the hashes will return the file as safe thereby defeating the purpose of anti-virus protection. Waldin takes it a step further by hashing the file, taking the size of the hashed file and comparing the size of the hashed file so that any alteration to the content of the file will be reflected in the size of the file.

On Page 3, applicant argues that the object that is forwarded to an output component in Waldin is scanned. Applicant claims that Waldin's examining of the authenticity of a digital signature of the file is the same thing as scanning of the file. Examiner respectfully disagrees. Waldin does not teach that authenticating the digital signature means scanning the file, in fact, Waldin point out the steps of authenticating the digital signature and in these steps, Waldin never mentions that the file is scanned before it is sent to the output component. Waldin goes on to teach that if the digital signature is authenticated the file is sent to the output component without scanning (Col 6, Line 65 thru Col 7, Line 3). If the digital signature is not authenticated, then the file has changed, only then does the whole process start from the beginning (Step 37) and the file is re-scanned and hashes taken and compared for virus infection.

In regards to claims 9 and 10, applicant argues that Waldin does not disclose updating a set of hash values based on a lack of a match. According to page 23, Lines 16-27 of applicant's specification, when the hash of an object is compared to the stored hash and no match is found (this is as a result of the object being infected or as a result of the object not having being previously scanned), the object is rescanned to determine if it is malicious and the new or updated hash value is stored for future comparison purposes. If any of these two conditions are present when the file is scanned, then the location where the hashes are stored is updated with the new hash of the file or the sector. Waldin anticipates these conditions and updates stored hashes based on the conditions. In Col 4, Line 4-16 and Line 45-67, Waldin teaches Module 3 of the system which stores the hash for a file or sector of a file when it is being scanned for the first time or when the contents of the file has changed. At the recipient computer in Col 6, Line 16-48 of Waldin, Module 5 does the comparison of the object to the stored hashes and if the values do not match, then it is determined that one of those two conditions are present, Module 5 then passes the object to Module 3 to rescan the file and update the stored hash in file 4.

In regards to claim 36, the Scan Module 3 of Waldin which contains anti-virus definition list anticipates the claim. In Col 6, Line 23-24, Waldin teaches that one of the jobs of the Scan Module 3 is to perform Step 37 which is to scan the file for viruses. Scan Module scans the file for viruses by comparing sectors of the file to a virus definition list (known objects in applicant's claim) in Col 4, Line 4-16 and Line 48-thru Col 5, Line 4, to determine if a virus is present in the file or the sectors of the file.

In view of the above explanation, examiner maintains the rejection because applicant's argument do not make the invention wholly and patentably distinct from the prior art disclosed by Waldin.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 4-6, 8-10, 17, 21, 24-25, 30-32, 34-38 and 41-43 are rejected under 35 U.S.C. 102(b) as being anticipated by Waldin et al. (US-6094731).

a. *Referring to claim 1:*

Regarding claim 1, Waldin teaches a method for filtering out exploits passing through a device (See Abstract), comprising:

receiving an object to be inspected directed to the device (Col 5, Line 51-52 teaches the recipient receiving a file);

determining a first hash value associated with the object to be inspected (See the response to argument and Col 2, Line 57-63 and Col 3, Line 21-34 and Col 6, Line 18-21 teaches determining a first hash value which is a hash of the size of the file);

determining a second set of hash values associated with objects that have previously been scanned (See the response to argument and Col 2, Line 57-63 and Col 3, Line 21-34 and Col 6, Line 18-21 teaches determining a second set of values which is a hash of the size of the file that has been previously stored);

if the first hash value matches at least one of the hash values in the second set, determining a third hash value associated with the object to be inspected (Col 6, Line 18-21 teaches comparing the hashes of the size of the file and Col 6, Line 37-42 teaches if they match, then determining a hash of the sectors of the file);

determining a fourth set of hash values associated with the objects that have previously been scanned (Col 6, Line 37-42 teaches determining the pre-stored hash of the sectors of the file); and

if the third hash value matches at least one of the hash values in the fourth set, immediately processing the object to be inspected (Col 49-52 teaches if the hash of the sector matches the pre-stored values, then immediately processing the file without scanning the file for virus).

a. *Referring to claim 4:*

Regarding claim 4, Waldin teaches the method of Claim 1, wherein the first hash value includes a rough outline hash value (ROHV) (Col 4, Line 63-65 teaches a hash of the size of the file as the ROHV).

a. *Referring to claim 5:*

Regarding claim 5, Waldin teaches the method of Claim 4, wherein the third hash value includes a sophisticated signature hash value (SSHV) and wherein the ROHV requires less time to compute than the SSHV (Col 4, Line 58-60 teaches the hash of the sectors of the file as the SSVH which requires more time to compute than the ROHV).

a. *Referring to claim 6:*

Regarding claim 6, Waldin teaches the method of Claim 1, wherein immediately processing the object further comprises forwarding the object to be inspected to an output component without scanning the object to be inspected (Col 6, Line 49-67 and Col 7, Line 1-3 teaches forwarding the file to the user or intended recipient without scanning the file if the comparison of the hash of the sectors match).

a. *Referring to claim 8:*

Regarding claim 8, Waldin teaches the method of Claim 6, wherein immediately processing the object to be inspected further comprises forwarding the object to be inspected to a destination (Col 6, Line 49-67 and Col 7, Line 1-3 teaches forwarding the file to the user or recipient without scanning the file if the comparison of the hash of the sectors match).

a. *Referring to claim 9:*

Regarding claim 9, Waldin teaches the method of Claim 1, further comprising if the first hash value does not match any of the hash values in the second set, scanning the object to be inspected for an exploit; and updating the second set of hash values to include the first hash value (See the response to argument and Col 6, Line 21-25).

a. *Referring to claim 10:*

Regarding claim 10, Waldin teaches the method of Claim 1, further comprising if the third hash value does not match any of the hash values in the fourth set, scanning the object to be inspected for an exploit; and updating the fourth set of hash values to include the third hash value (See the response to argument and Col, Line 42-45).

a. *Referring to amended claim 17:*

Regarding amended claim 17, Waldin teaches a system embodied on a computer storage medium encoded with a data-structure for protecting a device against an exploit Col 3, Line 47-67 and Col 4, Line 1-3), comprising:

a message tracker that is configured to determine whether an object has been previously scanned using a two-phase hash value technique (See Fig 1 and Col 6, Line 18-50 teaches the Antivirus accelerator module 5' determines if the object has been previously scanned using the two-phase technique), the two-phase hash value technique comprising:

determining a first hash value associated with the object (Col 2, Line 59 and Col 6, Line 19…. A first hash value of a file);

determining a second set of hash values associated with objects that have previously been scanned (Col 2, Line 60-61 and Col 6, Line 20-21… a stored hash value);

if the first hash value does not match at least one of the hash values in the second set, determining that the object has not been previously scanned (See Col 6, Line 37-39 teaches that the file is either infected or unscanned if the size hash doesn't match)

if the first hash value matches at least one of the hash values in the second set, determining a third hash value associated with the object (See the rejection in claim 1);

determining a fourth set of hash values associated with the objects that have previously been scanned (See the rejection in claims 1 teaching the pre-stored values as the hash values associated with the file);

if the third hash value does not match at least one of the hash values in the fourth set, determining that the object has not been previously scanned (See the rejection in claim 1); and

a scanner component that is coupled to the message tracker and that is configured to receive an unscanned object and to determine whether the unscanned object includes an exploit(See Fig 1 and Col 6, Line 18-50 teaches the Antivirus scan module as the scanner module which receives instruction from the accelerator module to scan the file if it includes an exploit).

a. *Referring to claim 21:*

Regarding claim 21, Waldin teaches the system of Claim 17, wherein the first hash value further comprises a ROHV (See the rejection in claim 1 and 4).

a. *Referring to claim 24:*

Regarding claim 24, Waldin teaches the system of Claim 17, wherein the third hash value further comprises a SSHV (See the rejection in claims 1 and 5).

a. *Referring to claim 25:*

Regarding claim 25, Waldin teaches the system of Claim 17, wherein the two-phase hash value technique further comprises:

if the third hash value approximately matches at least one of the hash values in the fourth set, determining that the object has been previously scanned (Col 6, Line 43-46 teaches if the sectors hash value doesn't match the pre-stored values, then the file is either infected or unscanned at which point the scan module scans it again).

a. *Referring to claim 30:*

Regarding claim 30, Waldin teaches the method of Claim 1, wherein: the first hash value and third hash value are determined by the device (Col 6, Line 10-55 teaches the first and third hash values are determined by the device); and

the second set of hash values and the fourth set of hash values are determined by the device based on previous scanning by the device (Col 6, Line 10-55 teaches the second and the fourth hash values are pre-stored values or hashes of previous scans).

a. *Referring to claim 31:*

Regarding claim 31, Waldin teaches the method of claim 1, wherein the method is performed by a firewall (Col 3, Line 21-28)

a. *Referring to claim 32:*

Regarding claim 32, Waldin teaches the method of claim 1, wherein the method is performed by a router (Col 3, Line 21-28).

a. *Referring to claim 34:*

Regarding claim 34, Waldin teaches the system of claim 17, wherein the system includes a firewall (Col 3, Line 21-28).

a. *Referring to claim 35:*

Regarding claim 35, Waldin teaches the system of claim 17, wherein the system includes a router (Col 3, Line 21-28).

a. *Referring to claim 36:*

Regarding claim 36, Waldin teaches a method comprising: receiving an object; matching a rough outline hash value (ROHV) of the object to ROHVs of known objects; if a match is found between the ROHV of the object to any of the ROHVs of the known objects, matching a sophisticated signature hash value (SSHV) of the objects to SSHVs of the known objects (See the response to argument and Col 4, Line 9-16 teaches the Scan Module 3 examining a file for virus by matching the file and sectors of the file to a virus definition list);

if a match is found between the SSHV of the object to any of the SSHVs of the known objects, processing the object as a malicious object; if a match is not found between either the ROHV of the object to any of the ROHVs of the known objects or the SSHV of the object to any of the SSHVs of the known objects, scanning the object (See the response to argument and Col 4, Line 9-16 teaches the Scan Module 3 examining a file for virus by matching the file and sectors of the file to a virus definition list); and if the scanning the object determines that the object is malicious, processing the object as a malicious object and updating the ROHVs of known objects and the SSHVs of the known objects (Col 4, Line 52-573 teaches the Scan Module 3 scanning the file for viruses and updating the virus definition list).

a. *Referring to claim 37:*

Regarding claim 37, Waldin teaches the method of claim 1, wherein the determining the first hash value includes determining a rough outline hash value (ROHV) based on a hash value of a first portion of the object (See the rejection in claims 1 and 4).

a. *Referring to claim 38:*

Regarding claim 38, Waldin teaches the method of claim 37, wherein determining the third hash value includes determining a sophisticated signature hash value (SSHV) based on a Message Digest 5, a Secure Hash Algorithm, or a Secure Hash Standard, and wherein the ROHV requires less time to compute than the SSHV (Col 1, Line 41-47 teaches common hash functions known in the art such as MD5, SHA-1 used in forming a hash of the file which requires more time to compute than the hash of the size).

a. *Referring to claim 41:*

Regarding claim 41, Waldin teaches the system of Claim 17, wherein the first hash value further comprises a ROHV determined based on a hash value of a first portion of the object (See the rejection in claims 1 and 4).

a. *Referring to claim 42:*

Regarding claim 42, Waldin teaches the system of Claim 17, wherein the third hash value further comprises a SSHV determined based on a Message Digest -5, a Secure Hash Algorithm, or a Secure Hash Standard (See the rejection in claims 1 and 38).

a. *Referring to claim 43:*

Regarding claim 43, Waldin teaches The method of claim 36, wherein: the ROHV is determined based on a hash value of a first portion of the object; and the SSHV is determined based on a Message Digest -5, a Secure Hash Algorithm, or a Secure Hash Standard See the rejection in claims 1, 37 and 38).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Waldin et al. (US-6094731), and further in view of Chen et al. (US-5960170)

a. *Referring amended to claim 33:*

Regarding claim 33, Waldin teaches the method of claim 1.

Waldin does not teach determining whether the file is compressed and if it is, decompressing the file.

However, Chen teaches determining if the object is compressed and decompressing the object if it is (See Chen, Col 15, Lines 5-13)

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to modify Waldin's system to determine if the file is compressed and to decompress it as taught by the Chen for the purpose of making the system more efficient in processing large files which have been compressed to a smaller size.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432